December 9, 2020 6:18PM EST

China: Big Data Program Targets Xinjiang's Muslims

Leaked List of Over 2,000 Detainees Demonstrates Automated Repression

© 2020 Badiucao for Human Rights Watch

(New York) – A big data program for policing in China's Xinjiang region arbitrarily selects Turkic Muslims for possible detention, Human Rights Watch said today. A leaked list of over 2,000 detainees from Aksu prefecture provided to Human Rights Watch is further evidence of China's use of technology in its repression of the Muslim population.

The big data program, the Integrated Joint Operations Platform (IJOP), apparently flagged the people on the Aksu List, whom officials then evaluated and sent to "political education" camps in Xinjiang.

"The Aksu List provides further insights into how China's brutal repression of Xinjiang's Turkic Muslims is being turbocharged by technology," said Maya Wang, senior China researcher. "The Chinese government owes answers to

the families of those on the list: why were they detained, and where are they now?"

Human Rights Watch first reported on the IJOP in February 2018, noting that the policing program aggregates data about people from various sensory systems in Xinjiang, and flags to officials those it deems potentially threatening. Officials then evaluate these individuals' "general performance" together with other sources of information, and send some to political education camps and other facilities. Human Rights Watch "reverse engineered" the IJOP mobile app in May 2019 and revealed the dubious criteria this mass surveillance system was programmed to flag, including many lawful behaviors.

The Aksu List, dated around late 2018, is similar to another leaked file, the Karakax List. That list–of people detained for having relatives abroad–dated around June 2019, provides an assessment of whether an individual should remain in detention. The IJOP is also repeatedly mentioned in the Karakax List. Together the lists provide two snapshots of Xinjiang's bureaucracy, as it picks and vets its victims in the process of coerced thought transformation: the decision to detain people and the decision to keep them in detention. At both stages, the IJOP system assists officials in selecting targets.

The entry for "Ms. T" on the Aksu List illustrates how the program's algorithms identify legal behaviors as grounds for detention. It notes that she was detained because the IJOP system had flagged her for "links to sensitive countries." It reported that Ms. T had received four calls from a foreign number in March 2017, down to the number of seconds. In other words, the IJOP system is programed to pick out particular behavior, calls to a foreign number, noting the precise duration of the calls. Human Rights Watch called that number and found that it belongs to Ms. T's sister.

Ms. T's sister said that Xinjiang police interrogated Ms. T around the time the Aksu List recorded her detention date. The police had specifically asked about her sister because she lives abroad. Ms. T's sister said she has had no direct contact with her family in Xinjiang since then, but heard via an intermediary that Ms. T—presumably upon her release from a political education camp—was now working in a factory five days a week and allowed to go home only on weekends. Ms. T's sister believes Ms. T is being forced to work in a factory against her will, noting that Ms. T had been training for a different career before she was detained.

Human Rights Watch's analysis of the Aksu List strongly suggests that the vast majority of the people flagged by the IJOP system are detained for everyday lawful, non-violent behavior. This contradicts the Chinese authorities' claims that their "sophisticated," "predictive" technologies, like the IJOP, are keeping Xinjiang safe by "targeting" criminals "with precision."

The mass surveillance and arbitrary detention of Xinjiang's Turkic Muslims violate fundamental rights under China's constitution and international human rights law. Article 37 of the constitution states that all arrests must be approved by either the procuratorate (the state prosecution agency) or the courts.

Yet Human Rights Watch research indicates that neither agency appears to be involved in these detentions. Rather, administrative officials, including police officers, make the sole decision to detain someone. Those facing detention have no right to due process, including access to lawyers and family members, or a chance to stand trial to contest such allegations. The use of intrusive surveillance, including in and around people's homes, also violates everyone's right to privacy.

“‘Predictive policing’ platforms are really just a pseudo-scientific fig leaf for the Chinese government to justify vast repression of Turkic Muslims,” Wang said. “The Chinese government should immediately shut down the IJOP, delete all the data it has collected, and release everyone arbitrarily detained in Xinjiang.”

The Aksu List:

May 1, 2019

China’s Algorithms of Repression

Reverse Engineering a Xinjiang Police Mass Surveillance App

Download the full report in English

Download the appendix of the report in English

لتنزيل الملخص والتوصيات بالعربية

Unduh ringkasan dan rekomendasi dalam [Bahasa Indonesia]

Télécharger le résumé et les recommandations en français

Descargue aquí el resumen y las recomendaciones en español

ئۇيغۇر تىلىدىكى قىسقىچە مەزمۇنى ۋە تەۋسىيەلىرىنى چۈشۈرۈڭ

Türkçe dilinde rapor özeti ve tavsiyeleri indirmek için tıklayınız

摘要和建议有中文版本

Authentication

In August, Radio Free Asia’s Uyghur Service provided Human Rights Watch with an Excel spreadsheet titled “List of IJOP Trainees” with the names of over 2,000 people obtained from an anonymous Xinjiang source in late 2018. The sheet has columns that include the person’s name, gender, the date of their detention in a political education camp, the reason for their detention, the number of their detention facility or cell, the batch number from which the IJOP systems picked them out, and the reason why, usually no more than a sentence or two.

Although the sender has not been identified, the list appears to come from a part of Aksu prefecture where 80 percent of the residents are Uyghurs. Human Rights Watch is confident that all the people on the Aksu List are Uyghurs. About half of the list are men and the other half women. Their detention dates ranged from mid-2016 to late 2018. At the peak, well over 100 people were detained on a single day. To protect the source, Human Rights Watch is obscuring the precise location of the Aksu List, precise dates, and some of the numbers throughout the analysis.

The file’s metadata suggests that it was last modified in late 2018. Human Rights Watch used various methods to verify the Aksu List:

- Human Rights Watch shared the Excel sheet with Uyghur diaspora communities from that region, who identified 18 names on the list as their immediate family members.

- The list also contains nearly 200 unique ID numbers, which were checked against the ID numbers on an official website of people who have been blacklisted under China's social credit system, run by the Supreme People's Court; and two of those numbers matched. The rate of 1 percent is consistent with the matching rate of those in the Karakax List, which contained more identifying personal information for extensive verification.

- Some entries say the individual was detained in a camp after completing a prison sentence, and 20 list the crimes. Human Rights Watch searched the Supreme People's Court's database of Chinese court verdicts for these 20 people's full names, but it did not yield results, though the court verdict database is far from comprehensive.

- The Aksu List also contains 27 unique Chinese mobile phone numbers. Human Rights Watch was able to find 14 of them on WeChat. In most cases, their photos, names, and locations indicate that they are Uyghurs from Aksu.

- The Aksu List contains two mobile phone numbers from outside China. One is still functional and, as noted, the person who picked up the phone confirmed she is the sister of the woman on the list we have called Ms. T.

The language and terms used in the Aksu List are also consistent with those in other Xinjiang official documents that Human Rights Watch reviewed. Human Rights Watch has shown the full Aksu List to two experts who have extensively documented Xinjiang's repression. They determined that the list appears authentic based on details such as detention duration and the language used.

The same Xinjiang source who provided the Aksu List also provided other audiovisual content to Radio Free Asia's Uyghur Service between mid and late 2018. Human Rights Watch analyzed this material to assess the credibility of the Excel spreadsheet, as it was obtained from the same source.

To protect the anonymous source, Human Rights Watch will not describe specifics of the analysis performed, but concluded that the audiovisual content was taken from inside a detention facility in Aksu. The embedded geographic coordinates suggest that they were taken from within a large building complex previously identified as a political education camp by the Australian Strategic Policy Institute, a think tank. This analysis provides Human Rights Watch with additional confidence in the authenticity of the Aksu List.

The Aksu List: Analysis

According to the Aksu List, the IJOP can flag people at both the prefecture and regional levels, though it is unclear how, or if, those two levels of analysis differ. At both levels, most people were flagged for their relationships, their communications (通联), or for being related to (家族人员 or 亲属), or traveling, or staying with (同行同住) someone the authorities consider suspicious. Column F appears to be the reasons officials give for detaining a person. An examination of the Aksu List suggests that the authorities consider the following behavior suspicious:

- Practicing Islam in the following ways:
    - Studying the Quran without state permission or allowing one's children to study the Quran;

    - Reciting the Quran, including Khitma [海提玛], the recitation of the entire Quran;
    - Preaching the Quran without state permission or listening to such preaching;
    - Wearing religious clothing, such as the burqa or veil, or having a long beard;
    - Having more children than allowed by China's family planning policy;
    - Marrying or divorcing outside of official Chinese legal requirements; for example, marrying before reaching the legal age (22 for men and 20 for women), marrying through a Nikah (an Islamic law marriage contract), or practicing polygamy;
    - Going on Hajj (the annual pilgrimage to Mecca in Saudi Arabia, considered a religious duty in Islam) without state permission;
    - Performing the Hijra (伊吉拉特), a form of migration to escape religious persecution following the pattern of the immigration of the Prophet Mohammed from Mecca to Medina in 622 CE, which the authorities consider to be motivated by adherence to Islam.
- Using suspicious (or "minority" 小众) software, in particular peer-to-peer file sharing application Zapya (快牙), but also Virtual Private Network, Skype, Payeco (易联), L2TP, and imo.
- Traveling:
    - Internationally to "sensitive" countries, including Turkey, Afghanistan, Saudi Arabia, and Kyrgyzstan;
    - Domestically outside Aksu, including elsewhere in Xinjiang such as Urumqi and Kashgar, or to other parts of China such as Beijing and Shanghai;
    - Without notifying local officials. People are also detained for having no fixed address.
- Going "off grid" (去向不明 or 轨迹不明), for example "switching off their phone repeatedly" or being missing for periods of time.
- Having mismatched identity, including using a cellphone number or ID card not registered in one's name, having more than one hukou (residency registration), or having falsified official documents like marriage certificates. In one case, losing an ID—subsequently used by someone else—was a cause for detention.
- Having "extremist thoughts" or downloading "extremist" audiovisual content.
- Having relatives in a group the authorities have labeled as terrorist, including the East Turkistan Islamic Movement (ETIM) and a couple of Aksu local groups.
- Having previously been a target of Xinjiang government actions, such as being detained or convicted of ordinary crimes or political crimes. In one case, a man was subjected to "political education" because he had been detained in 2014 for 15 days for carrying a knife and for not "properly explaining" the incident.
- Resisting official policies or official "management." In one case, a man was detained for not paying rent on his land.

- Being generally untrustworthy (不放心人员).
- Being young; that is, "born after the 1980s" (80, 90后不放心人员).
- "Generally acting suspiciously," "having complex social ties" or "unstable thoughts," or "having improper [sexual] relations."

In some cases, the alleged "problematic" behaviors dated to years earlier, revealing broad surveillance of legal and non-violent behavior going back decades. In one case, a man was detained for having studied the Quran in the mid-80s, and having "let his wife wear a veil" in the early 2000s. In another case, a woman was detained for once going to Kashgar, and once staying overnight in Hotan, both in 2013.

The authorities listed "terrorism" and "extremism," both perilously over-expansive terms in Chinese law, as the reasons for detaining about 10 percent (or over 200) of the people on the list. Yet the authorities did not allege that these detainees committed, incited, supported, or plotted any acts of violence, much less any acts that would rise to the level of terrorism. About one in five in this group were tagged for downloading or sharing "terrorism" or "extremism" content. About four in five were listed as being related to someone who had downloaded or shared such content, or to someone who was detained for terrorism or extremism. The Aksu List does not provide any additional information on the content of such audiovisual materials.

Governments may prosecute speech that incites criminal acts—speech that directly encourages the commission of a crime, is intended to result in criminal action, or is likely to result in criminal action—whether or not criminal action does, in fact, result. But laws that impose criminal punishment for what has been called "indirect incitement"—for example, justifying or glorifying terrorism—encroach on expression protected under international human rights law.

An examination of the Aksu List suggests that Xinjiang's Turkic Muslims are presumed guilty until proven innocent. In one case, a man was sent to political education camp because "suspicion [of him] cannot be eliminated and would require further interrogation." The evidence suggests that, consistent with official rhetoric, political education is akin to a form of preventive detention, where people's behaviors are deemed vaguely suspicious but not criminal. They are being held until their loyalty can be ascertained and, as needed, instilled.

Notably, three cases in the Aksu List suggest that people are treated with different levels of "strictness" depending on their level of obedience, and that people who disobey or "talk back" are placed in areas with stricter management. There appear to be three levels: "common management" (普管区), "strict management" (严管区), and "strong management" (强管区). The list also shows that some people are allowed to return home when they are sick (or in one case, breastfeeding), but are sent back to detention once they regain their health.

Human Cogs in the Machine

Previous Human Rights Watch research suggests that the IJOP system's requirements for officials to respond to many perceived abnormalities in people's lives is grueling. In mid-2019, Human Rights Watch was able to speak with an official in the region involved in carrying out the IJOP system. The person said:

> From 2016 to mid-2018 we were arresting people. In the beginning we were arresting those who spread terrorism videos, those who receive or give funds to ETIM, [and] those who participated in riots, and we would send them to the local political education centers. Later on ... there were quotas for arrests in all the locales, and so we began to arrest people randomly: people who argue in the neighborhood, people who street fight, drunkards, people who are lazy; we would arrest them and accuse them of being extremists. There was not enough room for them all in the centers, so they built new ones....

> In the beginning when the IJOP system came live, if [we] labeled someone as suspicious during evaluation, the local village committee and the police would go and take the person into custody. Later on, we rarely marked someone as suspicious. Often ... we asked them leading questions. Let's say we had to evaluate a person whom the system had lost track of. We'd [go to his home and] ask, "these last few days you were working the fields? You didn't go anywhere?" As long as they said yes, we'd fill out [the form in the app] noting the villager said he was working in the fields, he didn't go anywhere but everything was fine. It was like that for all other verification tasks."

The use of automation—which the authorities claim helps them identify those harboring the "ideological virus" of being disloyal to the Chinese Communist Party in a thorough and "precise" manner—can also lead to sloppy policing. The official said:

> [W]e wouldn't be able to finish the many verification tasks if we were to go through them all seriously.... But because we've been working [like this] for so long, whether it is our conscience or that we are tired, right now what's left [among officials] is just grievances and complaints; everyone wants to leave, nobody is doing this work properly.

Screenshots of the app made by a Xinjiang official showing the interface when populated with data (left), and alerts from the IJOP requiring that the official investigate individuals flagged by the system (right). © 2020 Private

Mission Creep

Information that has recently come to light from 2018 and 2019 suggests that the IJOP is used not only for picking out targets for detention, as described in the May 2019 Human Rights Watch report, but also to provide data for Xinjiang's larger government information system, that powers a range of government functions. This suggests that the authorities are increasingly sharing personal information across government agencies.

Government reports state that data collected via the IJOP system is also being used for a variety of vetting tasks,

from screening applicants for police jobs or public services such as poverty alleviation programs, to picking out model Communist Party members. Neither the initial collection of personal data nor the sharing and use of such data involve asking for consent, illustrating how powerless Xinjiang's residents are.

In Turpan County, for example, officials vet people using the IJOP system to select politically reliable people to take part in a "labor transfer" scheme; a program that involves organizing and transporting groups of Uyghurs to work in factories elsewhere in China under closely supervised, and often coercive, conditions. The same Turpan County scheme also draws on information gathered from "Physicals for All," another compulsory data collection program in which medical and health data is collected.

The integration of the IJOP system with other government systems, illustrates China's expansive definition of security and perceived need for extensive surveillance and control. In Xinjiang, the IJOP system is connected to information databases on second-hand cars, allowing the authorities to "compare information between persons and vehicles in real time, to discover suspicious clues in a timely manner, and to use information technology to effectively eliminate and prevent criminals from using second-hand vehicles to engage in various criminal activities that endanger the safety of society, as a publicly-available Xinjiang Department of Commerce notice says." The notice further explains:

> Each automobile trading hall in our region is equipped with ID card recognition devices and video image capture systems to examine the ID cards, residence permits, community certificates, convenient contact card, vehicle information ... of both buyers and sellers, to ensure that the person and their identity match. The information is uploaded to the Xinjiang Traffic Police Headquarters in a timely manner.

There is some preliminary evidence that the IJOP system itself is being used in China outside of Xinjiang. China Electronics Technology Group Corporation (CETC), the same company that built the IJOP in Xinjiang, built an IJOP system in Yinchuan, the capital of Ningxia province, says a procurement document dated January 2020 (for RMB 280.98 million, nearly US$43 million). CETC did not respond to a Human Rights Watch request for comment. Ningxia has the country's highest concentration of ethnic Hui, also a Muslim (though not Turkic) minority. While it is unclear how the system is being used, religious restrictions on Hui Muslims—closing mosques and Arabic-language schools, scrubbing Arabic scripts from Halal restaurants—have been on the rise in Ningxia and other Hui Muslim areas since 2019.

Your tax deductible gift can help stop human rights violations and save lives around the world.

$50	$100
$250	$500
$1000	Other
DONATE NOW	

Region / Country Asia, China and Tibet

Tags Mass Surveillance in China

Topic Free Speech, Religious Freedom, Detention Centers, Technology and Rights

MORE READING

December 4, 2020 | News Release

Hong Kong: Drop Cases Against Democracy Activists

December 3, 2020 | Commentary

China's Bully Tactics Haven't Silenced Australia

November 27, 2020 | Commentary

Biden Must Stand Up to China on Human Rights

REPORTS

May 1, 2019 | Report

China’s Algorithms of Repression

Reverse Engineering a Xinjiang Police Mass Surveillance App

MOST VIEWED

1 December 11, 2020 | Report

Armenia: Unlawful Rocket, Missile Strikes on Azerbaijan

2 July 29, 2020 | Report

“They Treated Us in Monstrous Ways”

3 December 11, 2020 | Report

Azerbaijan: Unlawful Strikes in Nagorno-Karabakh

4 December 10, 2020 | News Release

Saudi Arabia: Saudi-US Doctor Sentenced on Vague Charges

5 March 19, 2020 | Q & A

Human Rights Dimensions of COVID-19 Response

Protecting Rights, Saving Lives

Human Rights Watch defends the rights of people in 90 countries worldwide, spotlighting abuses and bringing perpetrators to justice

DONATE NOW

Get Updates On Rights Issues From Around The Globe

Enter an email address Sign Up

Connect With Us

Contact Us | Corrections | Privacy Policy | Permissions | Blackbaud Security Incident

© 2020 Human Rights Watch

Human Rights Watch | 350 Fifth Avenue, 34th Floor | New York, NY 10118-3299 USA | **t** 1.212.290.4700

Human Rights Watch is a 501(C)(3) nonprofit registered in the US under EIN: 13-2875808